process that progresses without external help. Modulus switching is another prominent strategy for achieving better asymptotic performance than bootstrapping.

- Step 4: Encrypted results are provided to client.
- Step 5: Client at its end computes decryption using decryption function and recovers f(message).

As a result no information is lost by getting encrypted results and decryption at its own end.

Motivation

Security is the key concern in cloud computing. Data provided to third-party service providers for processing and automation are a big issue. Every single business or organization wishes for the personal and sensitive data of the user. Every organization whether government, private, healthcare, academia requires data for policy formation, research purposes, planning new marketing strategies, or launching innovative products. Our main concern is with healthcare privacy as according to a survey by acumen research and consulting [1] healthcare cloud computing market will pass US$ 40 billion by the year 2026. Cloud computing in health care not only increases efficiency but also reduces cost. It is fast but protection of patient-sensitive data is the prime concern as it will not only promote patient confidence but also help in economic development. The digitization of a patient's medical records is supposed to improve care quality and efficiency while reducing costs. On the other hand, patient records include a considerable quantity of sensitive information. As a result, patients must be able to swiftly allow a range of medical affiliates to access their sensitive information using a simple, trustworthy, efficient, and secure approach. Therefore, it is vital to look at the usage of homomorphic encryption in healthcare and compare various homomorphic algorithms for illness prediction as well as data querying while protecting the privacy of patient information.

The rest of this article is organized as follows: the next section contains review methods, planning, inclusion and exclusion criterion, research questions with motivation. The subsequent section compares and analyzes homomorphic encryption starting with partial and somewhat homomorphic encryption approaches followed by fully homomorphic encryption approaches. Techniques to fully homomorphic encryption were classified into four categories, with significant approaches in each category were compared. The next section focuses on homomorphic encryption in the healthcare sector. Homomorphic encryption techniques were compared on the basis of communication and computation overhead for securely identifying LQTC, cancer, average heart rate, cardiovascular problems, and a secure query generating system in healthcare. Finally, conclusion is presented.

Review method

The systematic review process may be considered as a means of solving a specific research problem. Presently no systematic reviews are focusing on homomorphic cryptosystems in healthcare and bioinformatics, therefore a systematic review research methodology was chosen. As a result, the systematic review aims to close this significant research gap. Kitchenham and Brereton [2] recommendations were selected to evaluate and explain all homomorphic encryption research questions. Our work is motivated by the revolutionary work of Craig Gentry [3,4]. Additionally, the fact that fully homomorphic encryption will act as a boon to the healthcare industry as it will preserve complete privacy of patient health data is also a path of motivation. Reviewing the processes outlined in Fig. 2 will give a basic understanding of the systematic review process:

- ***Define research/review question:*** After reading various research/Journal articles and magazines and consulting with the expertise in the area of homomorphic encryption. Various research questions were identified.
- ***Develop Review Protocol:*** Pre-define the kind of research that will be included, as well as the procedures for collecting, evaluating, and analysing data.
- ***Identification of Research:*** After, Gentry's revolutionary work in homomorphic encryption, a number of homomorphic encryption methodologies in healthcare and bioinformatics were published. Despite tremendous research in homomorphic encryption there is no systematic review that considers quality of research and development.
- ***Extraction:*** Relevant research articles were included and irrelevant were excluded.
- ***Study Quality Assessment:*** Research articles were selected from popular repositories with keywords as homomorphic encryption to review basic homomorphic approaches.
- ***Data Synthesis:*** This phase entailed presenting data in descriptive and graphical form. It will help to make the overall evaluation of outcomes easier.
- ***Knowledge Translation:*** The findings and details of the review will be distributed to relevant target groups in a variety of media.

Review planning

The accomplishment behind each review depends on the selection of good-quality papers with unique work and genuine references. Thus, recognized journals, conference